UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/120,763	07/22/98	ETZEL M	ETZEL-5-3-11

LMC1/0620

PETER H PRIEST
529 DOGWOOD DRIVE
CHAPEL HILL NC 27516

EXAMINER	
SEAL, J	
ART UNIT	PAPER NUMBER
2766	5

DATE MAILED: 06/20/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. **09/120,763**	Applicant(s) **Etzel Et. Al.**
	Examiner **James Seal**	Group Art Unit **2766**

☒ Responsive to communication(s) filed on *Jul 22, 1998*

□ This action is **FINAL.**

□ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) *1-18* is/are pending in the applicat

Of the above, claim(s) ______ is/are withdrawn from consideration

□ Claim(s) ______ is/are allowed.

☒ Claim(s) *1-18* is/are rejected.

□ Claim(s) ______ is/are objected to.

□ Claims ______ are subject to restriction or election requirement.

Application Papers

□ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

□ The drawing(s) filed on ______ is/are objected to by the Examiner.

□ The proposed drawing correction, filed on ______ is □ approved □ disapproved.

□ The specification is objected to by the Examiner.

□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ______ .

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

□ Interview Summary, PTO-413

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: Page 3, lines 14 and 16, serial numbers should be included.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alanara (5594797), and further in view of Appendix A to IS-54 .

3. In claim 1, applicant recite a method which is to be employed with a wireless telephone encryption system in which a message is introduced, a first transformation is performed on the message, an iteration of the CMEA process is then performed employing an enhanced T-box function using an involutary lookup, the inputs of the enhanced tbox subject to permutation using one or more of the the secret offsets, and finally a second transformation is applied to the message to produce an output.

4. Alanara discloses a cellular telephone encryption system, which transforms plantext in a first stage, and an intermediate stage which the output of the first state is transformed by an involutary transformation and T-box and finally this results is transformed by a finally transformation (See Abstract Figures 5 and 6).

5. Alanara does not specifically mention the iteration of the CMEA, however, CMEA (Cellular Message Encryption Algorithm) is a standard in the Cellular Telecommunication Industry Association along see Appendix A to IS-54 pages 15 (See referencies cited but not applied). Iteration of the CMEA was also not mentioned by Alanara. Recently great concerns have been voiced about CMEA (see referencies cited but not applied). It would have been obvious for those skilled in the art to incorporate iteration of the CMEA and T-box lookup into Alanara's would greatly improve the security. Claim 1 is rejected.

6. In claim 2, applicant recites a method with the limitations of claim 1 and with the further limitations that there are one or more secret offsets.

7. Alanara discusses a cellular telephone system of the type discussed in claim 1, but does not disclose an offset for the tables. Appendix A, IS-54 page 4 and page 11, discusses two offsets and one skilled in the art would recognize use of a plurality of such offsets and making them secret would be an obvious extention of Alanara, especially with regards to the more recent securities over CMEA. Claim 2 is rejected.

8. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alanara and Appendix A, IS-54 as applied to claim 1 and 2 above, and further in view of Bruce Schneier.

9. In claim 3, applicant recites a method with the limitations of claim 2 and with the further limitations that the step of generating the first and second offset combine with a plurality of secret values with an external value.

10. The applicant's generation of secret table pointers (offset) in claim 3, in which the points are changed by a plurality of secret values with an external value, is an example of Vigenere autokeying (see Bruce Schneier, Vigenere ciphers, Chapter 1, Applied Cryptography) in which the keys are the pluality of secret values, and the external value is the plaintext. Claim 3 is rejected.

11. In claim 4 and 5, applicant recites the method of claim 3 with the further limmitation that the secret value includes two 8-bit values for each offset and further the external value is 8-bit value.

12. As is well known in the art 8-bits is one byte and if offset values are to be 1 byte of information, then any encyption of them should use at least 1 byte values (see Bruce Schneier, one time pad security, Chapter 1, Applied Cryptography). Claim 4 and 5 are rejected.

13. Claims 6-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alanara, Appendix A, and Schneier as applied to claims 4 and 5 above, and further in view of Vernan, and Friedman.

14. In claim 6, applicant recite the method of claim 5 with the further limitation that the offset 1 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$ and offset 1 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$.

15. To those skilled in the art, this is a well known means of taking two number strings and shifted them against one another to obtain a much longer string before the cycle repeats (see for example Vernam (AIEE Feb 1926, page109-115(in particular with Running ciphers page 113);W. F. Fridman (1522775) and (1516180); and Bruce Schneier, Chapter 1, Applied Cryptography). Claim 6 is rejected.

16. In claim 7, applicant recites a method which includes a first transformation including bit trading and involution lookup with feedback, radom byte permutation, each emploring secret offset.

17. Alanara, Schneier, and the IS-54 Appendix A involution lookup, random permultation, bit trading, and mading combinations of these depend on offset (Appendix A, page 6 and figure, Alanara Abstract, Schneier, Chapter 1, Applied Cryptography). Claim 7 is rejected.

18. In claim 8, applicant recites the method of claim 7 with the further limitation that a second transformation including bit trading and involution lookup with feedback, radom byte permutation, applied to each octet of the intermediate step, and each emploring secret offset.

19. Alanara, Schneier, and the IS-54 Appendix A involution lookup, random permultation, bit trading, and mading combinations of these depend on offset (Appendix A, page 6 and figure, Alanara Abstract, Schneier, Chapter 1, Applied Cryptography). Claim 8 is rejected.

20. In claim 9, applicant recites a method using the reverse enchance CMEA cryptoprocessing for each message in a call introducing a message to the system, creating more one or more secret offsets, performing a first inverse transform on unprocessed message, performing an iteration of the CMEA process on the first inverse tranformed message, employing T-Box function using involutary lookup, subject to permutation and secret offsets and a second inverse transformation to produce the final text.

21. Alanara discloses a cellular telephone encryption system, which transforms plantext in a first stage, and an intermediate stage which the output of the first state is transformed by an involutary transformation and T-box and finally this results is transformed by a finally transformation (See Abstract Figures 5 and 6).

22. Alanara does not disclose the use of a inverse enhanced CMEA, however the IS-54 Appendix discloses the CMEA and modified by the teaching of Schneier, Vernan, and Friedman, we notes that any cryptosystem transform must have an inverse and both must be present on communication device, in order to encrypt and decrypt incoming and outgoing messages, thus those skilled in the art would recognize that one could switch between the cryptographic transformations and its inverse (especially if not an involution) to double the number of possible encryption and thus increase the system security of the CMEA, which along is consider inscure. Claim 9 is rejected.

23. In claim 10, applicant recites a method with the limitations of claim 9 and with the further limitations that there are one or more secret offsets.

24. Alanara discusses a cellular telephone system of the type discussed in claim 9, but does not disclose an offset for the tables. Appendix A, IS-54 page 4 and page 11, discusses two offsets and one skilled in the art would recognize use of a plurality of such offsets and making them secret would be an obvious extention of Alanara, especially with regards to the more recent securities over CMEA. Claim 10 is rejected.

25. In claim 11, applicant recites a method with the limitations of claim 2 and with the further limitations that the step of generating the first and second offset combine with a plurality of secret values with an external value.

26. The applicant's generation of secret table pointers (offset) in claim 11, in which the points are changed by a plurality of secret values with an external value, is an example of Vigenere autokeying (see Bruce Schneier, Vigenere ciphers, Chapter 1, Applied Cryptography) in which the keys are the pluality of secret values, and the external value is the plaintext. Claim 11 is rejected.

27. In claim 12 and 13, applicant recites the method of claim 3 with the further limmitation that the secret value includes two 8-bit values for each offset and further the external value is 8-bit value.

28. As is well known in the art 8-bits is one byte and if offset values are to be 1 byte of information, then any encyption of them should use at least 1 byte values (see Bruce Schneier, one time pad security, Chapter 1, Applied Cryptography). Claim 12 and 13 are rejected.

29. In claim 14, applicant recite the method of claim 5 with the further limitation that the offset 1 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$ and offset 1 = $((K_0 + 1)*CS_n \bmod 257) \oplus K_1 \bmod 256$.

30. To those skilled in the art, this is a well known means of taking two number strings and shifted them against one another to obtain a much longer string before the cycle repeats (see for example Vernam (AIEE Feb 1926, page109-115(in particular with Running ciphers page 113); W. F. Fridman (1522775) and (1516180); and Bruce Schneier, Chapter 1, Applied Cryptography). Claim 14 is rejected.

31. In claim 15, applicant recites a method of claim 14 with the further limitation that includes a first inverse transformation including bit trading and involution lookup with feedback, radom byte permutation, each employing a first and second secret offset.

32. Alanara, Schneier, and the IS-54 Appendix A involution lookup, random permultation, bit trading, and mading combinations of these depend on a first and second secret offset (Appendix A, page 6 and figure, Alanara Abstract, Schneier, Chapter 1, Applied Cryptography). Claim 15 is rejected.

33. In claim 16, applicant recites the method of claim 15 with the further limitation that a second transformation including bit trading and involution lookup with feedback, radom byte permutation, applied to each octet of the intermediate step, and each emploring secret offset.

34. Alanara, Schneier, and the IS-54 Appendix A use a second transformation employing involution lookup, random permultation, bit trading, and mading combinations of these depend

on offset (Appendix A, page 6 and figure, Alanara Abstract, Schneier, Chapter 1, Applied Cryptography). Alanara does not disclose the use of a inverse enhanced CMEA, however the IS-54 Appendix discloses the CMEA and modified by the teaching of Schneier, Vernan, and Friedman, we notes that any cryptosystem transform must have an inverse and both must be present on communication device, in order to encrypt and decrypt incoming and outgoing messages, thus those skilled in the art would recognize that one could switch between the cryptographic transformations and its inverse (especially if not an involution) to double the number of possible encryption and thus increase the system security of the CMEA, which along is consider inscure. Claim 16 is rejected.

35. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alanara, Appendix A, Vernan and Friedman and Schneier as applied to claims 4 and 5 above, and further in view of James Reeds (5159634).

36. In claim 17 and 18, applicant recites a wireless handset for secure communication comprising a transceiver with input/output interface, key generator, cryptoprocessor with message identification, using forward enhanced iteration CMEA and first and second transformation, employing enhanced T-box, involutary lookup table, encryption/decryption processor and input/output interface for routing. Further he describes an associated wireless base station to compliment the wireless telephone.

37. Claim 17 is a device claim of the methods claims of 1-16, with the addition of the transceiver and interface making it a communication device. Claim 18 is the corresponding base

station that must compliment a wireless phone, to complete the system. Reeds decribes such a device (see for example figure 11). Those skilled in the art would be motivated to combine these teachings in order to have a working wireless telephone system. Claims 17 and 18 are rejected.

References Cited But Not Applied

38. The following references are cited but not applied. A number of articles have come out recently about the insecurity of the CMEA alone. For example David Wagner, Bruce Schneier, and John Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", May 30, 1997 and David Wagner, Bruce Schneier, and John Kelsey, "Flaw in Cell Phone Encryption Identified; Design Process Blamed" March 20 1997 have considered the details the CMEA, T-box lookup, etc. and in particular its cryptanalysis. The Patient by James Reeds, (5,159,634) and references listed therein, discusses much of the development of cellular telephone sercurity. Simon Avarne patent (5,371,796) December 6, 1994.

Conclusion

39. Any inquiry concerning this communication should be direct to James Seal at telephone number (703) 308 4562. The examiner can normally be reached on Monday through Friday from 7:30 a.m. to 5:30 p.m.

40. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703) 305-9711.

41. Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the Group receptionist, whose telephone number is (703) 305-3800. Fax number is (703) 305 0040.

James Seal

James Seal

12 June 2000

Gail Hayes

GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700